



Europäisches Patentamt
European Patent Office
Office européen des brevets



⑪ Publication number: 0 676 877 A2

⑫

EUROPEAN PATENT APPLICATION

⑬ Application number: 95301805.8

⑮ Int. Cl. 6: H04L 9/32

⑭ Date of filing: 17.03.95

⑯ Priority: 05.04.94 GB 9406615

⑰ Date of publication of application:
11.10.95 Bulletin 95/41

⑲ Designated Contracting States:
DE FR GB

⑳ Applicant: INTERNATIONAL BUSINESS
MACHINES CORPORATION
Armonk, NY 10504 (US)

⑷ Inventor: Holloway, Christopher J.
13 Wilder Close
Woking, Surrey GU21 3HA (GB)
Inventor: Matyas, Stephen Michael, Jr.
25 Valkill Drive
Poughkeepsie, New York 12601 (US)

⑵ Representative: Lloyd, Richard Graham
IBM (UK) Ltd,
UK Intellectual Property Department,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

④ Method and apparatus for authentication and verification of printed documents using digital signatures and authentication codes.

⑤ An apparatus 100 for authentication and verification of original document 110 is disclosed. The document contents are scanned and digitized, using a scanner 125. Then the encoded document contents are logically divided into segments containing data of a single type, and for each segment a set of authentication rules is identified. Thus apparatus 100 generates a digital signature of the document, applying a dual key security scheme to the digitized segments contents and to the secret key of the authenticator. Finally, an authentication code is printed on the document, including the digital signature and the encoded segments contents. To verify the authenticity, document 110 is scanned and digitized again and the digital signature is checked using the associated public key. If the check fails the verifier identifies which of the segment(s) has been modified, comparing it with the related encoded segment contents printed on the document to evaluate its validity.

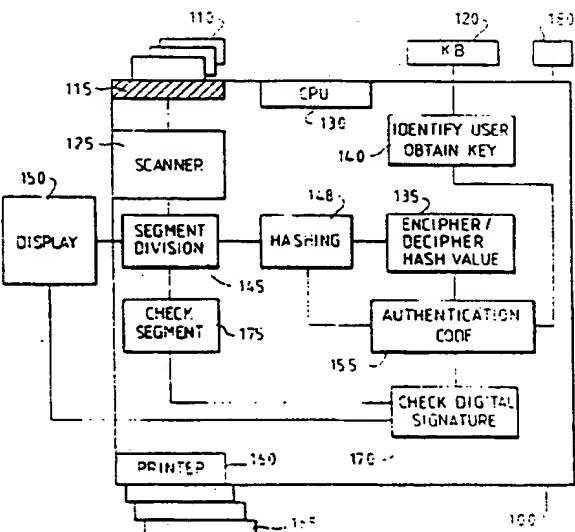


FIG. 1

This invention relates to the use of digital technology for allowing the authentication and verification of printed documents.

Despite the advance in modern computer technology, identification of people and the ownership of property is largely determined by paper documents. Many of these can be traded and themselves represent title in the sense of possession of the document grants title to the property. The documents are often accepted at different places and in different countries to their point of origin. Documents of their very nature get damaged and at some point the damage becomes so great that they can lose all value (e.g. they are destroyed by fire). Following such destruction, a copy of the original may be deemed to be the original, otherwise the copy should be distinguishable.

Traditionally, some authorized person, such as a notary or public officer, performs the authentication of the paper documents utilizing manual tools, such as affixing a signature, or a seal, or by using special paper which makes it more difficult to modify the written contents, e.g. the printing loses its original colour. However, with such methods the potential for fraud is considerable, and so the value of a more secure means of authentication is also very great. Techniques used to authenticate documents should be capable of being used in ways that are either intentionally copyable or intended to prevent copying by say photocopier, depending on the nature of the document.

A way of providing authenticated hard copy of a document using digital technology is described in US pat. no. 5,157,726. This patent describes a dual key or public key cryptosystem for making and authenticating a copy of an original document. In this system a hard copy of the original document is produced to which is added a public key digital signature which represents the document contents and the identity of the entity that supplies such hard copy. This patent also discloses a process for validating the authenticity of the signed hard copy, checking the digital signature and the hard copy document contents and indicating whether the signed copy is valid or invalid. The process for creating a digital signature is well known in the art, and is exemplified in international standards (viz. ISO 9796 and CCITT X509); it comprises processes of data reduction, for example hashing, and of encryption. There are several algorithms known in the art for both hashing and encryption that are suitable for the creation and verification of digital signatures.

However, some difficulties arise since the paper document is very susceptible to modification during its life, due to inkspot, partial erasure, dirt, writing added onto it, and other superficial damage. In such cases the document could still be deemed as valid, but the existing systems are not able to distinguish between such a damaged original document and unauthorized documents. In addition new problems may arise since the reading may not be reproducible. For example coded information, such as English sentences, can be read with reliability because interpretation can be put against each character and because words and sentence contain high degrees of redundancy; whereas it is more difficult against punctuation and spacing. Moreover non-coded information such as pictures and diagrams do not have these properties that permit analysis; similarly such reading is more susceptible to distortion through such superficial damage.

In accordance with the present invention is now provided apparatus for authentication of a document comprising means for generating and storing the contents of an original document in digital form, means to generate a digital signature from the digital form, and means to attach an authentication code to said original document for subsequent use in demonstrating the authenticity thereof, characterized by means for logically dividing of original document into segments, each segment containing data substantially of a single type, means to generate a digital form of each segment using a digitizing method suitable for the data type contained therein, the contents of each segment being reproducible from the digital form of the segment, and wherein said digital signature is generated from the digital forms of said segments, and said authentication code comprises the digital form of each segment and the digital signature.

This overcomes the problem of the prior art without any reduction of the security of document authenticity. In fact, any alteration of the paper document will modify the document contents which no longer correspond to the generated authentication code stored on it. The encryption of the digital form has the consequence that the code may not be generated by anyone not knowing the secret encryption key chosen; but, if a document fails verification then it is possible to compare the digital form of the original document, attached to the document, with the document itself to better evaluate if the check fails for a damage of the document or something else. In this way it is possible to generate an appropriate digital form for each type of data contained in the document such that the process of validation is improved since the system will be able to determine which segment or segments failed the check. Also this approach prevents compensating changes being made to two or more segments of the same document and obtaining a good overall verification. This attack is of particular concern where one segment may contain encoded information such as a photograph or a diagram which could be almost infinitely varied without noticeable change to the human eye; thus allowing pertinent textual changes to go unnoticed by the verification mechanism. Even so, the mechanism for obtaining a digital form of the content of the document, can be made sufficiently strong to render such attack infeasible.

Moreover, to demonstrate the authenticity of a paper document it is very useful that the authentication code attached is a true representation of its content, but scanners or other reading systems may not be very accurate and in a verification process this wrong representation could be compared with a properly read one.

5 In a preferred arrangement of the present invention, the apparatus comprises means for displaying each digital form and means enabling the digital form to be edited before said digital form is generated. This allows reading errors, which could invalidate a subsequent verification process to be corrected.

Moreover, the apparatus can comprise means to generate coordinates for locating each segment with respect to at least two different points on each page of said document, the coordinates being included in the digital form of each segment. This overcomes problems due to small changes in the orientation of the document. 10 between the process of authentication and the process of validation, which will cause such images to be represented very differently in binary form.

15 Other difficulties arise attaching the verification data to the document. Any authentication information stored upon the document must be stored so as not to be obtrusive. It must not interfere with the intended human usage of the document. However, if it is to be copyable it must also be printed in visible form and just finding space to print the information presents some difficulty. If it is not intended that the authentication information is copyable, then it can be printed invisibly making it unobtrusive and allowing many areas of the document to be used for storage. Alternatively, the authentication information can be stored outside of the document itself. In this case there needs to be a secure means of associating this with the material document.

20 Thus, the apparatus can comprise means to identify an area on said document wherein said authentication code may be attached. Preferably, the apparatus comprises means to print said authentication code and said at least two points on said document in a visible or invisible manner. This enables the printed documents to be copyable or not, according to the document requirements.

25 In a preferred arrangement of the present invention said means to generate a digital form of each segment can include means to generate a reduced form of each digital form, means to concatenate said reduced forms in a set and to reduce said set, and means to encrypt the reduced set and/or the reduced forms. This reduces the risks of compensating changes among the segment of the document, avoiding that the digital form of each segment is modified in accordance to a modification of the segment content on the document.

30 Preferably, the means to generate a digital form of each segment can comprise means for selecting the digitizing method suitable for the data type contained in the segment. This overcomes the problem of properly digitizing the data contained in the segment, reducing this complex step to a selection among a predefined list of sets of rules. In a particularly preferred arrangement of the present invention the digital signature is generated by a secret key of a public key authentication system. This feature improves the security by allowing a large group of people to verify such coded digital form and therefore verify the authenticity of the document. However only a person or a limited group of people have access to the secret key which may authenticate the 35 document by generating the encrypted form thereof.

35 Viewing another aspect of the present invention, there is also provided an apparatus for verifying the authenticity of a document provided with an authentication code comprising a first digital form of the document and a digital signature, said apparatus comprising means for generating and storing said document in a second digital form, characterized by means for decrypting said digital signature and storing said first digital form and said decrypted digital signature, said first digital form comprising the digital form of each segment in which the document is logically divided, and means for comparing said decrypted digital signature with said second digital form of said document, and each segment digital form of said first digital form with each segment of the document to verify the authenticity of said document.

40 An embodiment of the present invention will now be described with reference to the accompanying drawing in which:

45 Figure 1 depicts a block diagram of an apparatus for authentication and verification of original document.

Figure 2 depicts a segmented page of an original document.

Figure 3 depicts a block diagram of the authentication process of an original document.

Figure 4 depicts a process of definition of a segment of the document.

50 Figure 5 depicts a block diagram of the verification process of an authenticated original document.

55 In a system for authentication and verification of documents the authentication process should be able to verify the integrity of the document contents and to reduce the errors of evaluation. One of the known techniques for assuring integrity of data is through the use of cryptography, as often used for secure electronic transmission of data. One of the most acclaimed schemes uses the dual public/private key system and in this embodiment of the invention such principles are applied to authenticate and verify the document.

In this embodiment, the process of generating and verifying a digital signature is that known in the art. A signing authority possesses a secret key which may be used for encipherment, a verifying authority has access to the corresponding public key which may be used for decipherment. Data is first reduced in a hashing process.

using a publicly known hashing algorithm that requires no keys, to produce a hash value. The hash value is enciphered to generate a digital signature of the data. Verification is performed by recreating the same hash value from the original data, and recovering the hash value from decipherment of the signature. If the two hash values match then the data is deemed to be authentic. There are many approaches to controlling the usage of the secret key any of which would be suited to the present disclosure.

5 The general steps of the process are as follows:

- 1) The document contents are scanned, digitized, using a conventional scanner, and displayed page by page on a screen.
- 10 2) Using a conventional editor and an input device, such as a mouse, the signing authority identifies on the screen different segments of the document containing data of a single type and selects for each segment a set of rules, among a group proposed by the system, for authenticating it.
- 15 3) For each segment, a digital form of the data contents are derived using the method defined in the rules. A hash value of the rules used and the digital form of the segment contents is calculated using a public hashing algorithm.
- 4) A hash value for the document as a whole is obtained by calculating a hash value over the set of hash values for each segment.
- 15 5) The system, through a conventional input device, such as a keyboard or a card input device, receives the identification data of the signing authority and his secret signing key.
- 20 6) Applying one of many well known signing algorithms to the hash value of the whole document and using the secret signing key, the system generates the digital signature of the document.
- 7) The system prints the authentication code, containing the digital signature of the document, and the hash value, rules and digital form of each segments contents, on the document.
- 25 8) The authenticated document can then be transmitted to a verifying authority who obtains and verifies, or already possesses the public key counterpart to the secret signing key as part of this known public key or cryptography scheme. The public key may have been incorporated within the authentication code of the document in the form of a certificate such as defined in international standards (viz CCITT X509).
- 9) The document is scanned and digitized again, and for each segment a digital form is recreated and a hash for the segment calculated. The digital signature together with the public checking key are processed via a checking algorithm; this algorithm of which again a number are known, will determine whether or not the hash value of the document underlying the digital signature received corresponds to that obtained from calculating a single hash value across the set of hash values for each segment of the original document.
- 30 10) Since for each segment the verifier has access to both the locally calculated digital form and hash value, and to that carried in the authentication code, if the check fails, the user is able to identify which segment(s) have been modified or corrupted, and possibly what those modifications are, so that he will be in a better position for evaluating the validity of the document.

Referring first to Figure 1, it shows schematically one relatively simple apparatus 100 which has a space 115 for receiving a document 110 which may be an original document or an original authenticated document, a mouse 180 and a keyboard 120 for keying in appropriate commands and/or instructions to the apparatus where necessary, such as the information concerning the secret signing key and other information related to the identity of the user, which are checked in block 140. The apparatus has conventional optical reading means 125, such as a scanner, which preferably is combined to a conventional optical character recognition (OCR) unit which is capable of producing a digital form of the text character information presented on the document. The processing is controlled by a conventional programmable CPU 130, which for simplicity is not shown connected to, for example, keyboard 120 or scanner 125 or other modules employed in apparatus 100. The means to accomplish this would be clear to one skilled in the art. Then an image of the document generated from the digitized information is displayed on a screen 150 for the subsequent division into segments each containing data of a single type in block 145 and for each of the identified segments a method of encoding to create its digital form is selected. Then in block 148 each digitized segment is hashed. According to the digitizing method chosen each hashed segment and/or each digitized segment could be, optionally, signed in block 135. A digital signature is generated for the whole document by signing a hash value calculated over the set of hash values for each segment. Continuing with the description at block 155, the authentication code of the document is built by attaching the digital signature of the document to the hash values and digital forms of each of the segments. The digital signature is generated applying one of many well known public key signing algorithms and the secret signing key. In this case reference is made to the method disclosed in Meyer, Matyas "A new dimension in computer data security - CRYPTOGRAPHY", Wiley Interscience 1982, Chapter 9, particularly pp392-396. Finally, a printer 160 prints such authentication code on original document 165.

When document 110 is an authenticated document the function of the apparatus 100 is to make sure that the authentication code is valid. To do this, as previously described, the apparatus must obtain a valid copy

of the signer's public checking key, which is inserted in the system as described for the secret key, or preferably, it is read by the apparatus if printed on the document during the authentication process. The public key may itself be presented as a certificate which establishes its authenticity. Certification is well known in the art and is described for example in the CCITT X509 and ISO 9796 standards. Such a certificate would be verified by the verifier. In this case scanner 125, capable of reading and digitizing the contents of the document, will read also the authentication code contained in the document. Then a double check is performed. On one hand the digital forms of the segments contained in the authentication code are displayed for the verification process of each segment of the authenticated document at block 175; on the other hand, a hash is calculated for the digital form of each segment and compared with the segment hash included in the authentication code; and a single hash for the whole document is generated, as previously described, and it is compared at block 170 with the decrypted signature of the document, obtained from the digital signature using the public key.

Alternatively two different set of apparatus could be provided, one just for authenticating document and the other for verifying the authenticity of an authenticated document. In such a case, the device which provides the document verification process will have the same facilities as the authentication device, but does not have, or not use, the capability to print or sign.

Referring now to Figure 2 a typical page 200 of a document is shown. It contains many different forms of information: Text 230, a Letter head 220, a Logo 210, a Diagram 250, a Table 240, a Signature 260 and it could contain also pictures and images. In terms of information redundancy, significance, intelligibility, data decoding and repair each of these forms has very different properties and so is handled differently when reading the document. In fact any document can be digitized in any of several known ways. For instance if the document is wholly of text, it can be converted to a stream of ASCII codes and subsequently digitized; whereas reading the text may be insufficient to the process of ensuring authenticity when for example non-standard textual symbols are used, or non-textual, or graphical information is present in the document. In these cases the document can be digitized by known scanning process based on black/white or dark/light transition. Some identifiable points 270 are also inserted in page 200 and they are placed on the document during the process of authentication as described below.

Referring now to Figure 3, the document authentication process starts at step 300. In step 310 the document is inserted into the system; then, in step 320 all pages of the document are processed and page process 305 is performed for each page.

In step 315 page 200 to be processed is scanned and digitized, using a suitable scanner or an OCR system, for reading the content. Then in step 335 page 200 is subdivided into a set of segments 210, 220, 230, 240, 250, 260 and the coordinates of each segment are recorded and related to at least two defined and identifiable points 270 of the page 200. This allows that each page has a fixed position during the authentication process, avoiding small changes in orientation of the page during the validation process, which may cause the segments to be represented very differently in binary form.

These points 270 are called registration points and are printed on the document when it is first authenticated. Registration points 270 are placed as far apart as possible, but not so close to the edge of the paper as to get lost or damaged. They are also placed so as not to interfere with the other content of the document and for redundancy, it is preferable to have more than two points 270 in case one is lost. In step 345 the authorities system presents page 200 on the screen with suggested placement for registration points 270, if not already present, and suggested segments. An editor is provided, which allows the user to identify on the screen, using a mouse 180 or the keyboard 120 as in a conventional wordprocessor, the different segments of the document. In step 348 the authorizer agrees or modifies the suggested information. Then in step 355 all the segments are processed and for each segment, segment process 308 is performed. Whilst in the present case the definition of the segments is performed by the user on a displayed image of the document, the possibility that this may be performed automatically via recognition of a particular features of the segment is not excluded.

In step 328 the system displays the proposed system definition 210, 220, 230, 240, 250, or 260 for the segment.

Referring now to Figure 4, the user selects on the screen from a scroll bar menu 420 of a menu bar 440 the set of authentication rules, which will be applied to each single segment 400, among a group of default type based upon the category of information in the segment which could be changed for each instance. Otherwise, the user may decide to define a new set of rules since for example some paragraphs may be essential to the value of the document and must be strongly authenticated, and others may be allowed to be repaired, or might not need authenticating at all. To do that, the user selects the 'Define' action from the scroll bar menu 430. Then he defines a new name for the new set and he highlights in a table 410, containing all the existing authentication rules, the ones useful for providing his goal. Such highlighted rules will become the new set of authenticated rules identified by the new name. Then the new name is inserted in scroll bar menu 420 for the

selection. In the same way it is possible to update an existing set of rules. For example, if the user wants to modify the set named 'Formula', he has to select 'Modify' on the scroll bar menu 430, then he selects 'Formula' from the scroll bar menu 420 and at the end he highlights new rules or unhighlights any of the old one. With the option 'Delete' of the scroll bar menu 430, it is possible to delete one of the defined set, selecting it in the scroll bar menu 420. However, the set of authentication rules from which to choose must be common to the scheme as a whole, and the selected rule for each segment must be clear to the verifier, and could be defined within the segment definition of each segment. A list of the default authentication rules for the different types of segment is now provided:

- 5 Logos The authorizer types the name of the company whose logo is on the document. This information is included in the segment definition and is presented for verification when the document is to be checked.
- 10 Text The system decodes the text into ASCII, including capitalization, punctuation and spaces. However, a series of spaces is reproduced to a single space; and line feeds are ignored. The coded form should be displayed to the authorizer along with the image of the same text from the document so that the user may verify the text. Any identified spelling or context error in the decoded data is highlighted as these may represent decoding errors. The user then repairs the decoded data so as to be a true representation of the document content. The repaired data is authenticated.
- 15 Tables Vertical and horizontal division lines are removed by the imaging system under the control of the user. The coordinates of all removed lines are recorded in the segment definition. The data content of the table is treated as text.
- 20 Images This data includes also Pictures, Diagrams and Signatures. It is the most difficult as it often cannot be reliably coded. An image is taken of the segment to a particular imaging standard that is defined in the segment definition. If the image is to be authenticated, as in the case of a person's photograph or signature, then the image is compressed an compressed form stored within the segment definition, then the compressed form is authenticated. For a verification of an image, two options exist: either the decompressed form is displayed along the scanned segment. These are compared and any differences are highlighted. The user checking the document can then make an assessment of the significance of any differences;
- 25 alternatively, a statistical form of validation can be performed using techniques applied to biometric identification, yielding a probability that this is the original image.
- 30 In both cases the authenticator verifies the reference pattern used in the comparison.

Referring back to figure 3, in step 348, the authorizer accepts the presented segment definition and authentication rules or modifies them. Thus, the content of the segment is encoded using the authentication rules. Now, the process moves to step 368, where the coordinates, rules and digital form of the segment are hashed to give a hash value for the segment; the hash value, the coordinates, the authentication rules of the segment and the digital form are included in the segment definition.

Now, the control is transferred again to step 355, which checks if other segments of the page are still waiting to be processed; if not, in step 365 the page definition is built and hashed. Therefore the page as a whole is reduced by taking the hash values of the segments and of the page in turn and creating a hash of the concatenated set.

Clearly the above steps would not be necessary for each instance, or segment, of a defined document type such as a passport, but would be defined once and incorporated within the authentication system of the issuing authorities. However the definition would be made available to any verifying authorities, and this could be done, as further described, by carrying the information on each document of that type, or defining the verification system independently.

After the completion of step 365 the control passes to step 375, wherein the page is scanned again, unless it is still held securely within the apparatus, and in step 385 the suggested placements for the segment definition and the hash values are verified to be available. Thus in step 395 the page and the segments definitions and the page hash value are printed on the same page or, when identified, in the additional papers or stored in the associate storage means. It will be understood that any available method for encoding digital data on paper may be used. An example of such a technique is described in UK patent application no. 2,218,240A.

The control is now returned to step 330, which checks if other pages of the document are still to be processed; if not, in step 340 the signing authority agrees to the document definitions, as built during the process, and in step 350 he provides to the system his secret key of a dual key security scheme for a validity check. If the key is still valid the signing authority is authorized to sign the document, thus, in step 360, the document as a whole is authenticated by taking the hash value of each page in turn and creating a hash of the new concatenated set, finally this document wide hash is signed by the signing authority, using his secret key. In step 370 the page of the document which contains the suggested placement for printing the digital signature is scan-

ned again, unless it is still held securely within the apparatus, and in step 380 said suggested placement is verified to be available. The authorization process ends in step 390, printing the digital signature on the document.

Those skilled in the art will appreciate that the stream of digital information representing the document contents can be simply subjected to a checksum or similar algorithm or function whose output would then represent the actual full contents of the document, instead of hashing as described above, but that this would provide less protection against intentional modification. Similarly, all the digital information can be digitally signed before attaching it on the paper to increase the security of the document. Moreover, the digital information may be attached to the document in any of several known ways such as printing or sticking.

In this example the digital signature is attached to the document by being printed in a visible manner on the document itself using a suitable method for encoding digital data on paper. However it will be appreciated that the signature could be printed invisibly, which prevents the digital signature from being photocopied; or could be printed on a separate piece of paper or stored in other storage means which is secured to the document. In the case of invisible printing the scanning equipment will scan both the visible and the invisible content, and it will present the two sets of information preferably in different positions, or displaying them using different styles of the font or colours, so that the verifying user can associate them easily without one set interfering with the other. For verification of the hash values, the signature, and the segment definitions, which include segment contents, authentication rules and coordinates of the segment, representing the authentication code of the document, must all be retrieved from the document itself or an associated storage medium. This data is subject to the same reliability difficulties as the document content. However, each discrete set of information can be protected against accidental damage by the inclusion of simple check codes (e.g CRC) or sophisticated error detection and repair codes of known type; and in verification process, authentication data too should be allowed to be repaired by the authorized user so that document validation may proceed.

Referring now to Figure 5, the verification process starts at step 500. In step 510 the document is inserted into the system; then, in step 520 all pages of the document are processed and for each page, page process 505 is performed. In step 515 page 200 to be processed is scanned, for reading all the content, visible or invisible. In step 525 the authentication code stored into the document is read and the page hash and the segment and page definitions are identified, for allowing the complete process of the page. In step 554 all the segment definitions of the page are processed and for each of them segment process 508 is performed.

In step 518 the image of the encoded content of the segment, contained in the segment definition, is rebuilt and displayed on the screen, and in the meantime, reading the segment coordinates and the segment authentication rules contained in the same segment definition, also the actual content of the segment is displayed on the screen. Those skilled in the art may appreciate that the two images may be overlapped for a better evaluation of the differences, or the system itself may highlight such differences. In step 538 the contents of both the representations may be edited to improve the verification process, allowing the verifier to repair the data damaged or wrongly read in one of the two representations, based on the data contained in the other representation. Clearly this step could be prevented, or limited, for some kinds of document or data. In step 558 the actual content of the segment, repaired or not, is hashed, as already described in step 368, and in step 568 this derived hash is compared with the hash code of the corresponding segment registered on the document. If part of the authentication code is damaged, and if the verifying user is permitted to repair it, then the repaired authentication code is substituted for the changed one only during this verification process. For security reasons, the verifying user is not provided with any capability to update the authentication code stored on the document. Obviously, depending on the kind of the damage, part of the authentication process should be carried out again to produce the repaired authentication code. However, it is never permissible to repair the digital signature of the document as a whole.

At the end of step 568, the control is returned to step 545, which checks if other segments are still to be processed; if not, in step 555 the actual content of the page is hashed, as explained in step 365, and in step 565 the resulting hash code is compared with the hash code of the correspondent page registered on the document, repair to the page hash being allowed in the same way as repair to the individual segment hashes. The control is now returned to step 520 which checks if other pages are still to be processed, if not in step 530, the verifier accepts the content of the document as read, and repaired, by the system. Then in step 540 the verifying user inserts the public key certificate corresponding to the secret key used for authenticating the document. This is verified in step 550 the accepted content of the document is hashed, as explained in step 360. The process ends in step 560, wherein the document hash obtained from the digital signature is compared with the hash produced by verifying the document. If both are equal then the document is accepted.

As mentioned previously, there are many ways by which the various functions described above can be implemented, and the invention is not limited to the specific means by which the digitalization, optical reading, comparison system and other authenticating and verifying features are implemented.

Claims

1. Apparatus for authentication of a document (110) comprising means (125) for generating and storing the contents of an original document in digital form, means to generate (135, 155) a digital signature, and means (160) to attach an authentication code to said original document (110) for subsequent use in demonstrating the authenticity thereof,
 5 characterized by:
 means (145) for logically dividing the original document into segments, each segment containing data substantially of a single type;
 10 means to generate a digital form of each segment using a digitizing method suitable for the data type contained therein, the contents of each segment being reproducible from the digital form of the segment, and wherein said digital signature is generated from the digital forms of said segments, and said authentication code comprises the digital form of each segment and the digital signature.
- 15 2. Apparatus as claimed in claim 1 comprising means (150) for displaying each digital form and means enabling said digital form to be edited before generating said authentication code.
- 20 3. Apparatus as claimed in any previous claim, comprising means to generate coordinates for locating each segment with respect to at least two different points on each page of said document, wherein the coordinates are included in the digital form of each segment.
- 25 4. Apparatus as claimed in any previous claim, comprising means to identify an area on said document wherein said authentication code may be attached.
5. Apparatus as claimed in any previous claim, comprising means (160) to print said authentication code and said at least two points on said document in a visible or invisible manner.
- 30 6. Apparatus as claimed in any previous claim, wherein said means (145) to generate a digital form of each segment include means (148) to generate a reduced form of the digital form of each segment and means to concatenate the reduced form of the segments in a set and to reduce said set, means to encrypt the reduced set and/or the reduced forms.
- 35 7. Apparatus as claimed in any previous claim, wherein said means (145) to generate a digital form of each segment comprises means for selecting the digitizing method suitable for the data type contained therein.
8. Apparatus as claimed in any previous claim, wherein the digital signature is generated using a secret key of a dual key authentication system.
- 40 9. Apparatus for verifying the authenticity of a document (110) provided with an authentication code comprising a first digital form of the document and a digital signature, said first digital form comprising the digital form of each segment into which the document (110) is logically divided, said apparatus (100) comprising means (125) for generating and storing said document in a second digital form, characterized by:
 means (125, 170) for reading the digital signature and first digital form of the document from the document, decrypting said digital signature and storing said first digital form and said decrypted digital signature, and
 45 means (170, 175) for comparing said decrypted digital signature with said second digital form of said document, and said first digital form segment by segment with the document to verify the authenticity of said document.
- 50 10. Apparatus as claimed in claim 9 comprising means (150) for displaying and correcting the first digital form segment by segment to verify the authenticity of the authenticated document.
11. Apparatus as claimed in claim 9 wherein said means (170) for decrypting the authenticated form use a public key verifying the authenticity of a document provided with an authentication code by apparatus as claimed in claim 8.
- 55 12. Apparatus, as claimed in any of claims 1 to 8, comprising an apparatus as claimed in any of claims 9 to 11.

13. Method for authentication of a document comprising the steps of generating and storing the contents of an original document in digital form, encrypting said digital form to generate a digital signature, and attaching an authentication code to said original document for subsequent use in demonstrating the authenticity thereof, characterized by the steps of:

5 logically dividing the original document into segments, each segment containing data substantially of a single type;

selecting a digitizing method suitable for the data type contained in each segment, generating a digital form of each segment, and in that said authentication code comprises the digital form of each segment and the digital signature.

- 10 14. Method for verifying the authenticity of a document provided with an authentication code comprising a first digital form of the document and a digital signature, said first digital form comprising the digital form of each of a number of segments into which the document is logically divided, said method comprising the steps of generating and storing said document in a second digital form, characterized by the steps of:

15 reading the digital signature and first digital form of the document from the document,

decrypting the digital signature,

storing said first digital form and said decrypted digital signature,

comparing said decrypted digital signature with said second digital form of said document, and said first digital form segment by segment with the document to verify the authenticity of said document.

20

25

30

35

40

45

50

55

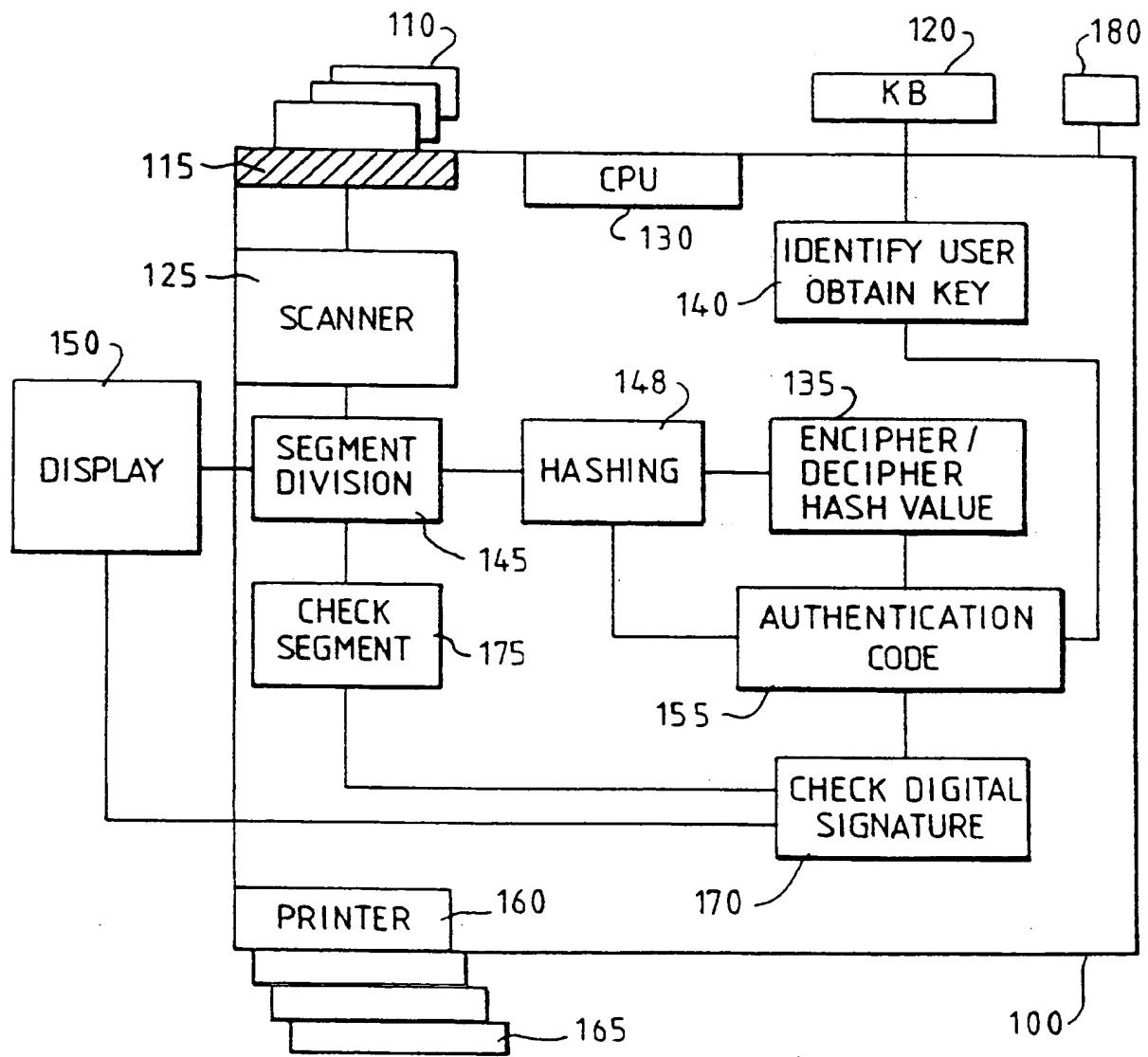


FIG. 1

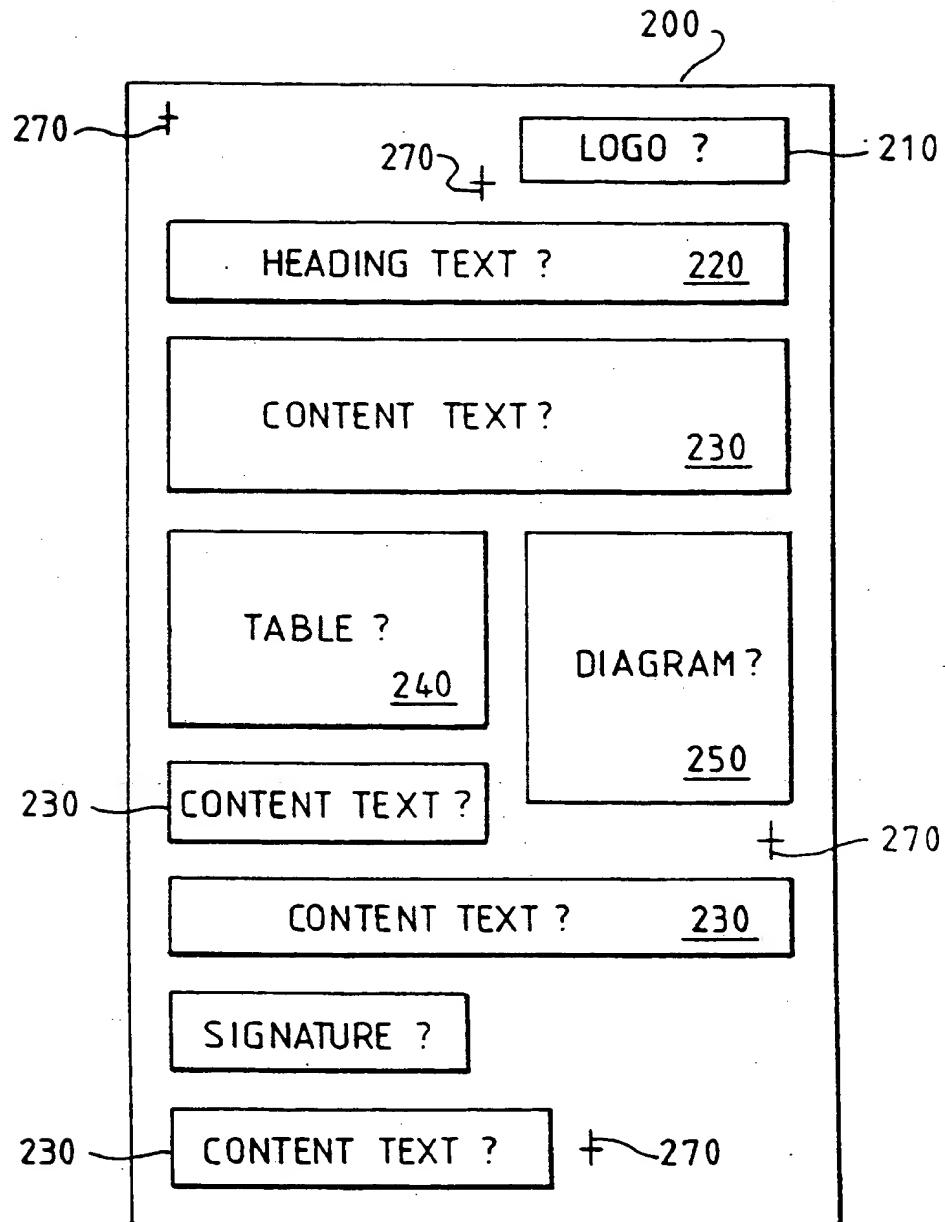


FIG. 2

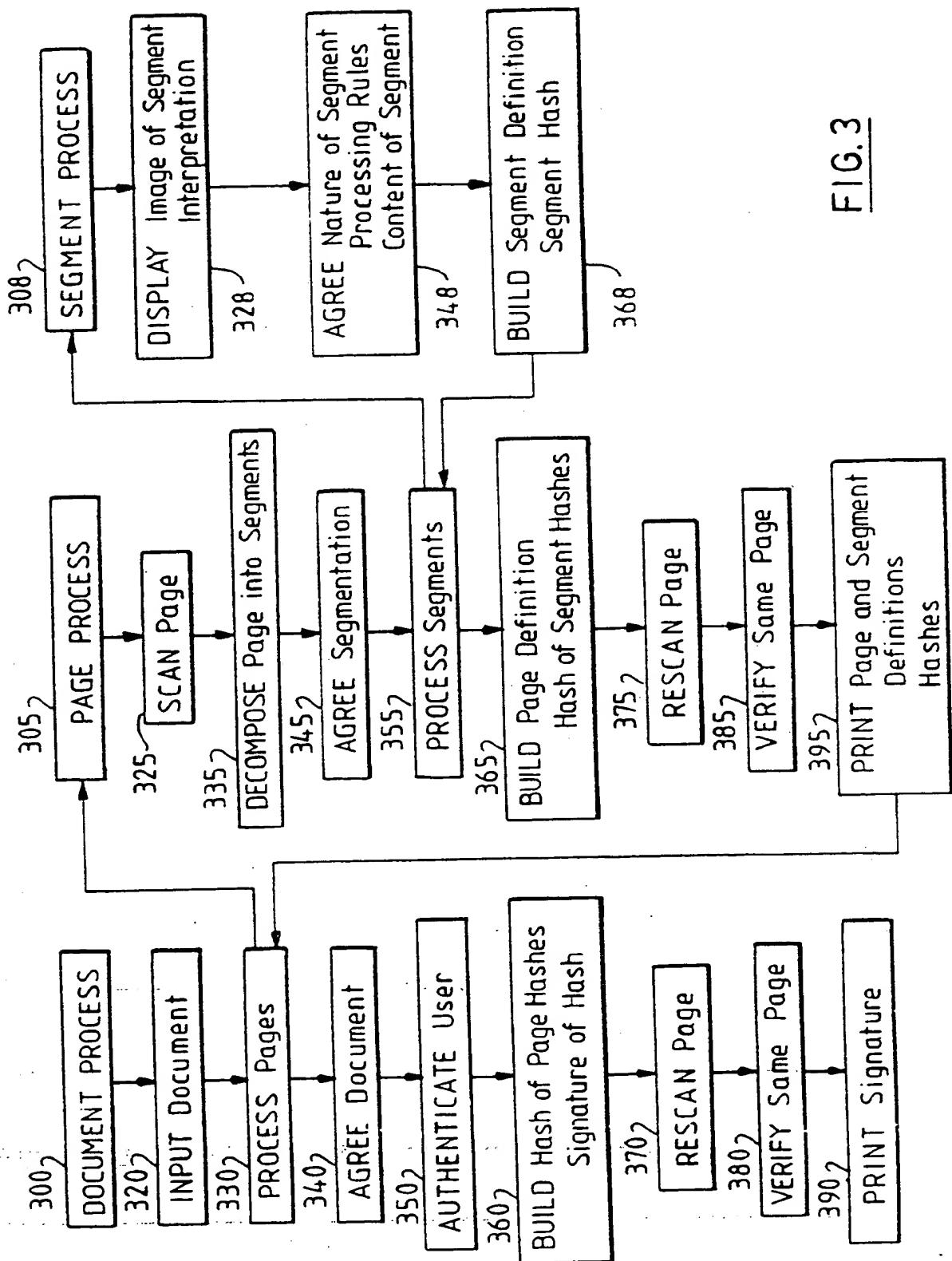


FIG. 3

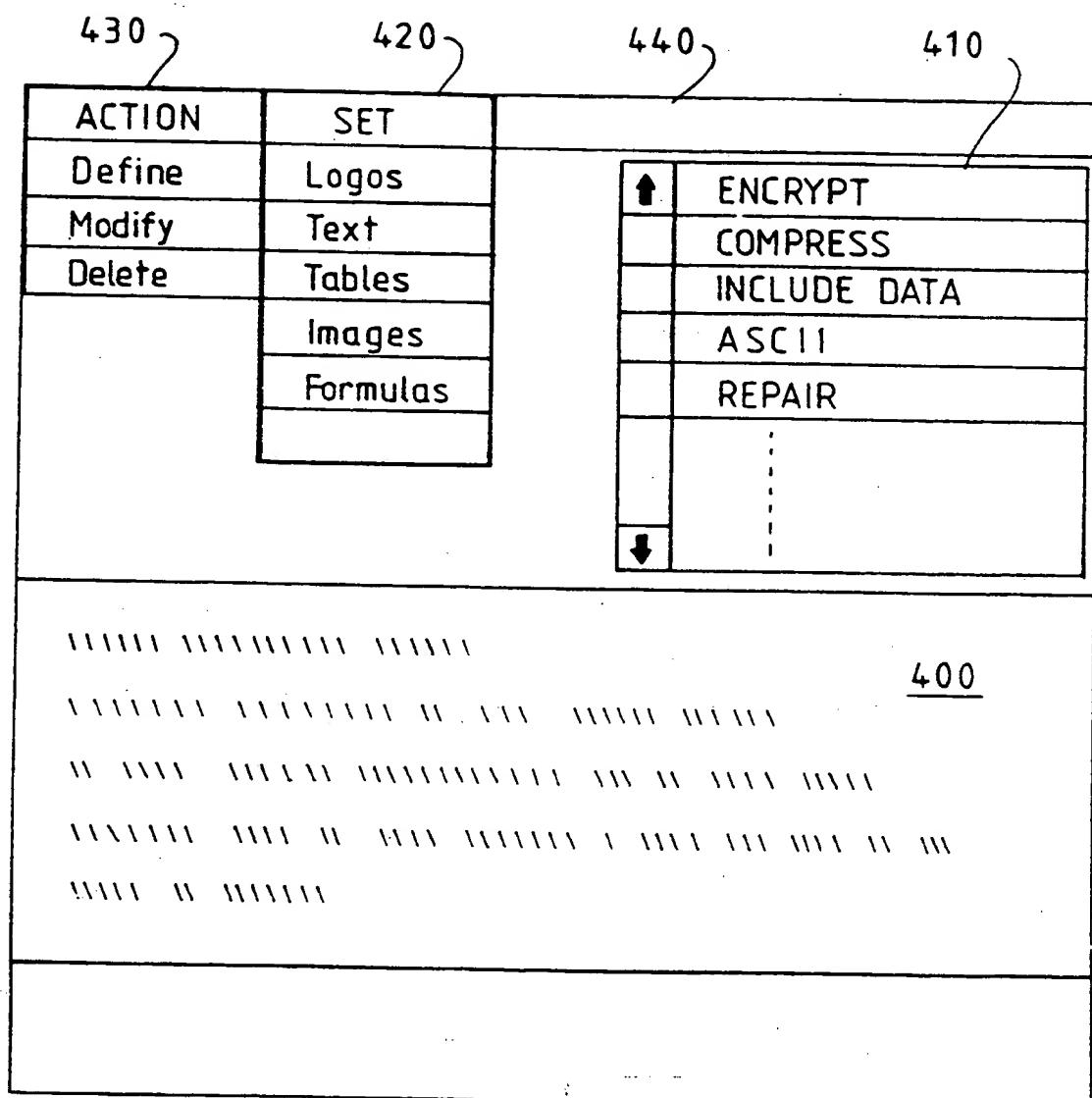


FIG. 4

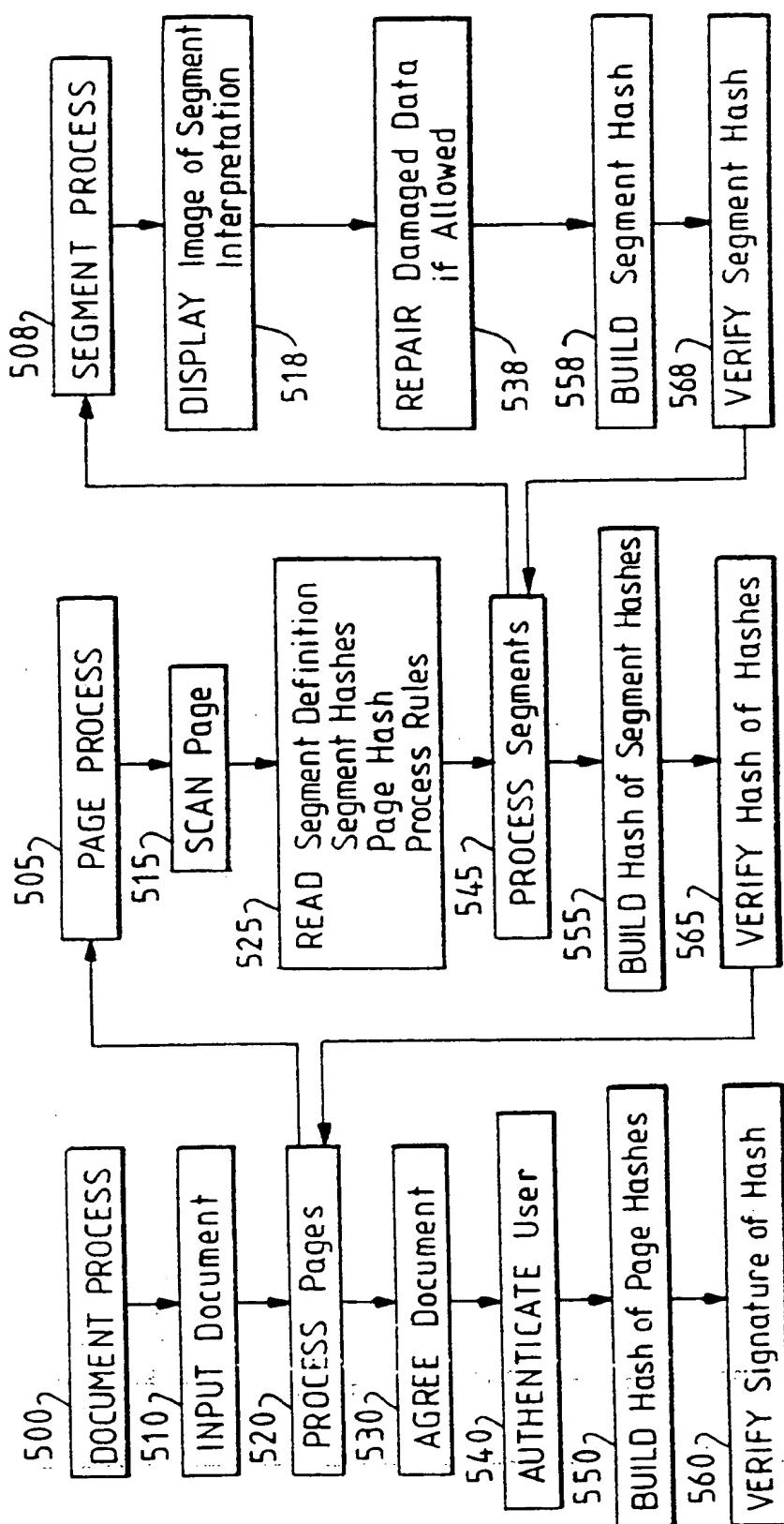


FIG. 5